SEESTADT BREMERHAVEN

Rahmenrichtlinie zur Informationssicherheit beim Magistrat der Stadt Bremerhaven

In-Kraft-Treten: 01.01.2025

Impressum:
Magistrat der Stadt Bremerhaven,
vertreten durch den Oberbürgermeister Melf Grantz
Postfach 21 03 60
27524 Bremerhaven

Hausanschrift Verwaltungszentrum (Stadthäuser 1 - 6):
Hinrich-Schmalfeldt-Straße
27576 Bremerhaven

Telefon: 0471 590-0
E-Mail: Stadtverwaltung at magistrat.bremerhaven.de

Verantwortliche Dienststelle:
Magistratskanzlei
Hinrich-Schmalfeldt-Straße 42, 27576 Bremerhaven

Inhalt

1 Einleitung

Die Verwaltungsabläufe in den Organisationseinheiten (Ämter, Amtsstellen und Referate) des Magistrats der Stadt Bremerhaven sowie der Sondervermögen (Eigen- und Wirtschaftsbetriebe) und der Anstalten des öffentlichen Rechts werden mittlerweile weitgehend durch den Einsatz von Informationstechnik (IT) unterstützt und sind somit von ihr abhängig.

Durch die verstärkte Abhängigkeit von moderner IT hat sich das Risiko der Beeinträchtigung von Informationsinfrastrukturen und deren IT-Infrastruktur-Komponenten durch vorsätzliche Angriffe von innen und außen, durch fahrlässiges Handeln, Unkenntnis oder technisches Versagen sowohl qualitativ als auch quantitativ deutlich erhöht. Mangelnde Informationssicherheit kann zu Störungen bei der Aufgabenerfüllung führen, die Leistungsfähigkeit der Stadtverwaltung mindern und im Extremfall die Geschäftsprozesse zum Erliegen bringen.

Ein unzureichendes Sicherheitsniveau oder Sicherheitslücken können über die Netzinfrastrukturen wesentliche IT-Verfahren negativ beeinträchtigen. Es ist davon auszugehen, dass die gestellten Sicherheitsanforderungen im Bereich der Informations- und IT-Sicherheit künftig weiter steigen werden.

Vor diesem Hintergrund ist die Sicherstellung der Informationssicherheit für den Magistrat der Stadt Bremerhaven eine der zentralen Aufgaben, in deren Rahmen ein angemessenes Sicherheitsniveau in den Geschäftsprozessen organisiert werden muss.

In dieser Rahmenrichtlinie zur Informationssicherheit werden die geltenden grundlegenden Ziele und Regelungen der Informationssicherheit festgelegt.

Die Rahmenrichtlinie zur Informationssicherheit:

- orientiert sich an den allgemeinen Sicherheitsstandards, wie dem IT-Grundschutzkonzept des Bundesamtes für Sicherheit in der Informationstechnik (BSI),
- beschreibt den Stellenwert der Informationssicherheit,
- legt den Geltungsbereich fest,
- enthält das Bekenntnis der Amts-, bzw. Betriebsleitungen zu ihrer Verantwortung für die Informationssicherheit,
- legt die Sicherheitsstrategie fest,
- formuliert die allgemeinen Sicherheitsziele,
- definiert die Sicherheitsorganisation,
- verpflichtet zur kontinuierlichen Fortschreibung des Regelwerks zur Informationssicherheit und
- legt den Rahmen zur Inkraftsetzung und Veröffentlichung fest.

2 Geltungsbereich

Die Rahmenrichtlinie zur Informationssicherheit gilt für alle Organisationseinheiten des Magistrats der Stadt Bremerhaven sowie für die Sondervermögen der Stadt Bremerhaven und die Anstalten des öffentlichen Rechts, soweit sie an das Verwaltungsnetz (Magistratsnetz) angeschlossen sind.

Sie gilt somit nicht für das pädagogische Netz der Schulen, das Netz der Ortspolizeibehörde Bremerhaven, das Schulungsnetz der Volkshochschule (VHS) sowie das Netz der Integrierten Regionalleitstelle Unterweser-Elbe.

3 Stellenwert der Informationssicherheit

Die Informationssicherheit nimmt in Zeiten der fortschreitenden Digitalisierung der Datenverarbeitung, der zunehmenden Vernetzung sowie der steigenden Bedrohung durch Risiken und Angriffe einen immer höheren Stellenwert ein.

Eine funktionierende Verwaltung ist heute ohne elektronische Kommunikationsmedien und IT-Verfahren nicht mehr denkbar.

Beim Einsatz von IT muss darauf geachtet werden, dass der Sensibilität von übertragenen und verarbeiteten Informationen und Daten mit der nötigen Sorgfalt Rechnung getragen wird. Dies hat ebenso für analoge Informationen und Daten Gültigkeit. Denn Informationssicherheit umfasst nicht nur IT-Systeme, sondern auch Papierunterlagen in Form von Akten und sonstige Daten im allgemeinen Sinn.

Die Informationssicherheit ist eine unverzichtbare Grundlage für ein Verwaltungshandeln, dem die Bürger:innen, die Wirtschaft und alle weiteren Partner:innen ihr Vertrauen schenken. Im Bereich der Informationsverarbeitung und Kommunikation müssen deshalb Verfügbarkeit, Integrität und Vertraulichkeit sowie Datenschutzanforderungen der verarbeiteten und übertragenen Informationen durch angemessene technische und organisatorische Maßnahmen gewährleistet werden.

Die Informationssicherheit ist ein unverzichtbarer Grundwert. Gründe hierfür sind insbesondere:

- Die gesetzlichen Vorschriften, beispielsweise zum Datenschutz, müssen eingehalten werden. Dienst- und Amtsgeheimnisse müssen gewahrt bleiben.
- Dienstleistungen für Bürger:innen, Wirtschaft und Verwaltung müssen sicher, zuverlässig und vertrauenswürdig erbracht werden.
- Die Auswirkungen eines Schadensfalls sind durch angemessene Vorsorgemaßnahmen zu minimieren.
- Die in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte müssen erhalten werden.
- Ein Ausfall der IT kann die Verwaltung in ihrer Arbeitsfähigkeit lahmlegen bzw. stark einschränken.
- Unbefugt veränderte oder gelöschte Daten können zu finanziellen Verlusten und evtl. zu Regressansprüchen führen.
- Die Verletzung der Sicherheitsziele kann zu deutlichen Ansehens- und Vertrauensverlusten führen.

4 Informationssicherheitsstrategie

Die Sicherheitsstrategie der Stadtverwaltung Bremerhaven ist es, mit wirtschaftlichem und personellem Ressourceneinsatz ein angemessenes Maß an Sicherheit zu erreichen und verbleibende Restrisiken zu minimieren. Die Sicherheitsstrategie wird durch die schrittweise Einführung eines Informationssicherheitsmanagementsystems (ISMS) realisiert.

Die Sicherheitsstrategie umfasst die gesamte Informationsverarbeitung im Geltungsbereich. Das ISMS soll dem jeweiligen Schutzzweck angemessene Sicherheitsmaßnahmen definieren und für deren wirtschaftliche Umsetzung sorgen.

Bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen ist darauf zu achten, dass das erforderliche Sicherheitsniveau erreicht wird, ohne den Ablauf von Geschäftsprozessen unnötig zu beeinträchtigen. Die Sicherheitsstrategie wird von den folgenden Grundsätzen der Informationssicherheit geprägt:

- Sicherheit für nachhaltige Verfügbarkeit: Um eine langfristige Verfügbarkeit zu erreichen, ist eine kurzfristige Einschränkung bei Funktionalität und Komfort vertretbar.
- Prinzip des Schutzbedarfs: Der Schutzbedarf von IT-Systemen wird vom Schutzbedarf der darauf verarbeiteten, gespeicherten oder übertragenen Daten bestimmt.
- Minimalprinzip des Zugriffs: Der Zugriff auf IT-Systeme und Daten wird auf die notwendigen Personen und Systeme beschränkt.
- Restriktives Nutzungsprinzip: Alle Nutzer:innen erhalten nur die Zugriffsrechte, die sie zur Erfüllung ihrer Aufgaben benötigen.
- Einbindung aller Beschäftigten: Alle Beschäftigten werden in den Sicherheitsmanagementprozess zur Unterstützung der Sicherheitsstrategie eingebunden und hinsichtlich der Informationssicherheit sensibilisiert.
- Zentrale Rolle der Informationssicherheit: Die Informationssicherheit wird bei Änderungen und Neuerungen von Beginn an mitberücksichtigt. Der/die Informationssicherheitsbeauftragte ist bei allen Fragen zur Informationssicherheit zu unterstützen.
- Verhältnismäßigkeit der Sicherheitsmaßnahmen: Aufwand und Ergebnis der eingesetzten Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zueinanderstehen.
- Bereitstellung von ausreichenden Ressourcen: Um ein angemessenes Maß an Informationssicherheit zu erreichen und aufrechtzuerhalten, sollen ausreichende finanzielle, personelle und zeitliche Ressourcen bereitgestellt werden.
- Soweit weitere Regelungen zur Informationssicherheit erarbeitet werden, geschieht dies stets auf Grundlage dieser Rahmenrichtlinie.

5 Ziele und Grundsätze der Informationssicherheit

Ziel ist es, die Informationen und IT-Systeme in ihrer Verfügbarkeit so zu sichern, dass es zu keinen Stillstandzeiten und Datenverlusten kommt. Auch gilt es, die Integrität und Vertraulichkeit von sensiblen Daten des Personals und der Bürger:innen im gesetzlich vorgeschriebenen Umfang zu garantieren.

Schadensfälle mit finanziellen Auswirkungen und immaterielle Folgen in Form von Imageschäden für den Magistrat der Stadt Bremerhaven müssen verhindert werden.

Die Informationssicherheit orientiert sich an folgenden drei Grundschutzzielen:

- Vertraulichkeit
  - Informationen dürfen ausschließlich einem berechtigten Personenkreis zur Verfügung stehen. Informationen sind vor unbefugter Preisgabe und Kenntnisnahme zu schützen.
- Verfügbarkeit
  - Systeme, Anwendungen und Daten müssen den berechtigten Personen in jeder Situation wie vorgesehen zur Verfügung stehen.
- Integrität
  - Die Korrektheit (Unversehrtheit) von Informationen und die korrekte Funktionsweise von Systemen ist sicherzustellen. Eine Verletzung der Integrität liegt vor, wenn Daten selbst oder Metadaten unerlaubt verändert werden oder unvollständig sind. Die physische und logische Unversehrtheit von Systemen, Anwendungen und Daten muss jederzeit gewahrt sein.

Bei der Erreichung dieser Ziele ist eine Verhältnismäßigkeit der eingesetzten Mittel zum Wert der schützenswerten Güter zu beachten.
Belange der Informationssicherheit sind von Beginn an zu beachten bei:

- der Planung, Konzeption und Einführung von Fachverfahren,
- der Prüfung der Auswirkungen auf die Gestaltung von Organisation und Arbeitsabläufen,
- dem Betrieb und der Administration von Fachverfahren,
- der Beschaffung und der Entsorgung von IT-Produkten,
- der Zusammenarbeit mit anderen Behörden einschließlich Nutzung von Diensten Dritter sowie
- der Aus- und Fortbildung von Beschäftigten.

6 Informationssicherheitsmanagement (ISM)

Informationssicherheit ist kein unveränderbarer Zustand, sondern ein Prozess, der ständigen Veränderungen unterworfen ist. Verwaltungsprozesse und Fachaufgaben können sich ebenso ändern wie gesetzliche Rahmenbedingungen.

In diesem Sinne wird sich nicht nur darauf beschränkt, ein einmalig erstelltes technisch-organisatorisches Sicherheitskonzept adäquat umzusetzen. Nach der Umsetzung ist auch regelmäßig darauf zu achten, ob die dokumentierten Sicherheitsmechanismen überhaupt in dem geplanten Umfang wirksam sind und ob diese unter dem Aspekt der Angemessenheit nicht ggf. noch effektiver gestaltet werden können. Auch gilt es, Überregulierungen zu vermeiden bzw. rückgängig zu machen. Änderungen müssen wiederum geplant und umgesetzt werden. Insgesamt müssen die Sicherheitsmaßnahmen im Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen und wirtschaftlich vertretbar sein.

Die Richtlinien zur Informationssicherheit in der Stadtverwaltung Bremerhaven sind hierarchisch aufgebaut. Die Rahmenrichtlinie zur Informationssicherheit ist die oberste Richtschnur. In der Richtlinie für den Aufbau der Informationssicherheit werden die grundlegenden Anforderungen und Maßnahmen des Informationsschutzes beschrieben.

Hinzu kommen weitere Dokumente (Richtlinien, Konzepte, Dienstanweisungen), die diese Anforderungen detailliert für die verschiedenen Verantwortlichen, Rollen oder Sicherheitsbereiche konkretisieren. Sie sind nicht Bestandteil dieser Rahmenrichtlinie, haben sich aber auf die Vorgaben aus dieser Rahmenrichtlinie zu beziehen.

Zum Zeitpunkt des Inkrafttretens dieser Rahmenrichtlinie sind folgende Richtlinien mit erlassen worden:

- Richtlinie zum Umgang mit Daten und IT-Systemen
- Richtlinie Internet Nutzung
- Richtlinie für die Nutzung der elektronischen Post
- Richtlinie zum Umgang mit Software
- Richtlinie zum Umgang mit Passwörtern
- Richtlinie zur IT-Sicherheit

Eine Übersicht über alle gültigen Richtlinien ist im Intranet unter Verwaltung und Recht / Recht / Dienstanweisungen und Richtlinien zu finden.

7 Informationssicherheitsorganisation

Um das erforderliche Sicherheitsniveau zu erreichen, zu halten und fortzuentwickeln, wird im Geltungsbereich nachfolgend beschriebene Informationssicherheitsorganisation etabliert.

7.1 Informationssicherheitsbeauftragte/r

Durch Magistratsbeschluss ist unter Einbindung der Mitbestimmungsgremien mind. ein Informationssicherheitsbeauftragter / eine Informationssicherheitsbeauftragte bestellt, der/die die dienstellenübergreifende Informationssicherheit und IT-Sicherheit in den Organisationseinheiten des Magistrats der Stadt Bremerhaven sowie den Sondervermögen und den Anstalten des öffentlichen Rechts überwacht.

Der/die Informationssicherheitsbeauftragte zeichnet verantwortlich für den Informationssicherheitsprozess und koordiniert die Informationssicherheit in der Stadtverwaltung. Dieser Prozess hat das Ziel, ein ressortübergreifendes Informationssicherheitsmanagementsystem (ISMS) zu etablieren, aufrechtzuerhalten und kontinuierlich zu verbessern.

Er/sie hat ein direktes Vortragsrecht bei der Betriebsleitung des Betrieb für Informationstechnologie (BIT) und bei der Magistratsdirektorin/dem Magistratsdirektor. Er/sie unterrichtet beide mindestens einmal jährlich über aktuelle Risiken sowie über die Wirksamkeit des ISMS und der getroffenen Sicherheitsmaßnahmen.

Im Einzelnen handelt es sich hierbei um:

- Planung, Koordination, Steuerung und Dokumentation des Informationssicherheitsprozesses,
- Fortschreibung der Rahmenrichtlinie zur Informationssicherheit,
- Erstellung und Fortschreibung von Sicherheitskonzepten, Notfallvorsorgekonzepten sowie weiterer Richtlinien und Regelungen zur Informationssicherheit,
- Mitwirkung an der IT-Strategie und IT-Architektur des Magistrats,
- Erstellung von Berichten an den Magistrat,
- Untersuchung sicherheitsrelevanter Vorfälle von erheblicher Bedeutung,
- Initiierung und Steuerung von Angeboten für Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit, in Zusammenarbeit mit der Fortbildungsabteilung des Personalamtes,
- Unterstützung der behördlichen Datenschutzbeauftragten bei der Freigabe automatisierter Verfahren zur Verarbeitung personenbezogener Daten,
- Planung, Durchführung, Auswertung sowie Nachbereitung und ggf. Beauftragung von IT-Sicherheitsaudits (Risiko- und Schwachstellenanalyse).
- Mitwirkung beim CERT Nord (Computer Emergency Response Team) der Freien Hansestadt Bremen

Zur Unterstützung des/der Informationssicherheitsbeauftragten wird eine Arbeitsstruktur geschaffen, die es ermöglicht, die Informationssicherheit in den beschriebenen Bereichen weiter auszubauen.

Zur Umsetzung der Informationssicherheitsorganisation und Unterstützung der Organisationseinheiten leitet der/die Informationssicherheitsbeauftragte eine Arbeitsgruppe der Fachadministrator:innen.

7.2 Lenkungsausschuss IT-Sicherheit

Für die Steuerung und Lenkung des Informationssicherheitsmanagements ist der Lenkungsausschuss zuständig. Dem Lenkungsausschuss gehören an: die Magistratsdirektorin/der Magistratsdirektor, die Betriebsleitung des BIT und die Leitung der Abteilung Informations- und Kommunikationstechnik der Magistratskanzlei.

Als Berater nimmt an den Sitzungen der/die Informationssicherheitsbeauftragte teil.

Er/sie bereitet notwendige Änderungen an der Struktur der Informationssicherheit für den Magistrat vor und berichtet nach Beschlussfassung in geeigneter Form der AG IT-Strategie.

8 Verantwortlichkeiten und Rollen

8.1 Betrieb für Informationstechnologie (BIT)

Der BIT ist, im Auftrag des Magistrats, dafür zuständig, die für die im Geltungsbereich benannten Organisationseinheiten über den BIT zur Verfügung gestellten Clients, Netz- und Serverinfrastrukturen sowie sämtliche Basisdienste so auszulegen, dass eine hohe Vertraulichkeit und Integrität sowie eine hohe Verfügbarkeit der verarbeiteten Daten garantiert werden kann, die der Sensibilität der verarbeiteten Personal- und Bürgerdaten in vollem Umfang entspricht. Die IT-Administrator:innen des BIT besitzen im Hinblick auf die IT-Sicherheit eine besondere Verantwortung.

8.2 Verantwortung der Leitung

Die Verantwortung für die ordnungsgemäße und sichere Aufgabenerledigung und damit für die Informationssicherheit haben die Leitungen der Organisationseinheiten sowie der Sondervermögen und der Anstalten öffentlichen Rechts.

Die vorgenannten Leitungen sind zuständig für die Einhaltung der Rahmenrichtlinie. Die Aufgaben und Pflichten des BIT sind in einem Vertrag zur Auftragsdatenverarbeitung detailliert definiert.

Die Leitungen können die Aufgabenerledigung auf die für die einzelnen Fachverfahren jeweils zuständigen Fachverantwortlichen delegieren. Hierzu gehört grundsätzlich die Nutzungsverwaltung einschließlich der Zugriffsrechte auf der Ebene der Fachverfahren.

8.3 Verantwortung der Fachadministrator:innen

Die Fachverantwortlichen richten die Zugangs- und Zugriffsrechte in dem Fachverfahren im Rahmen der vom Informationseigentümer/ der Informationseigentümerin festgelegten Berechtigungen sowie behördenspezifische Verfahrenseinstellungen ein. Sofern externe IT-Dienstleistende mit der Administration von Fachverfahren beauftragt werden, sind die Vorgaben aus der Rahmenrichtlinie zur Informationssicherheit zu beachten.

Sofern Fachverfahren der Freien Hansestadt Bremen oder anderer Bundesländer oder des Bundes eingesetzt werden, haben die Fachverantwortlichen sicherzustellen, dass deren Vorgaben zum Betrieb der Fachverfahren umgesetzt werden. Dazu sind die einzuleitenden Maßnahmen auf Client- oder Netzwerkebene mit dem BIT abzustimmen.

Fachadministrator:innen für einen Geschäftsprozess oder ein IT-Fachverfahren sind zuständig für:

- die Festlegung der geschäftlichen Relevanz seiner Informationen und deren Schutzbedarf und
- die Sicherstellung, dass Verantwortlichkeiten explizit definiert und Sicherheits- und Kontrollmaßnahmen zur Verwaltung und zum Schutz seiner Informationen umgesetzt werden.

Sofern keine Fachverantwortlichen benannt wurden, obliegen die hier beschriebenen Aufgaben den unter 8.2 genannten Leitungen.

8.4 Berechtige Personen der Organisationseinheiten

Im Zusammenhang mit erweiterten Berechtigungen zum Beantragen von Basis- und erweiterten IT-Diensten dürfen, durch die unter 8.2 genannten Leitungen die Berechtigungen zur Beantragung an bestimmte und festgelegte Mitarbeiter:innen übertragen.

8.5 Verantwortung der Beschäftigten

Die Beschäftigten im Geltungsbereich haben eine hohe Verantwortung für Informationssicherheit und die IT-Sicherheit. Insbesondere tragen sie eine hohe Verantwortung für die Vertraulichkeit der Daten und halten die relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein. Sie sind es, die in der täglichen Verwaltungspraxis die organisatorischen und technischen Vorgaben umsetzen müssen.

Jede Person kann durch verantwortungs- und sicherheitsbewusstes Handeln dabei helfen, Schäden zu vermeiden und zum Erfolg beizutragen. Sensibilisierung für Informationssicherheit und fachliche Schulung der Mitarbeiter:innen sind daher eine Grundvoraussetzung für Informationssicherheit.

Die Beschäftigten müssen über den Sinn von Sicherheitsmaßnahmen aufgeklärt werden. Dies ist insbesondere wichtig, wenn sie Komfort- und/oder Funktionseinbußen zur Folge haben. Die Sicherheitsmaßnahmen sollten für die/den Anwender:in transparent und verständlich sein, sofern dadurch kein Sicherheitsrisiko entsteht.

Alle Beschäftigten sind ferner verpflichtet, Sicherheitsmängel und identifizierte Bedrohungen umgehend den Informationssicherheitsbeauftragten zu melden und aktiv an deren Beseitigung mitzuarbeiten.

Beabsichtigte oder grob fahrlässige Verletzungen der Informationssicherheit sind zum Beispiel:

- Der Missbrauch von Daten.
- Der unberechtigte Zugriff auf Informationen oder ihre Änderung oder unbefugte Übermittlung.
- Die nicht autorisierte Nutzung von Informationen.
- Die Gefährdung der Informationssicherheit Dritter.
- Die Zerstörung oder der Diebstahl von Informationen oder Informationsressourcen.

Bei Verstoß gegen diese Rahmenrichtlinie oder weitere Richtlinien, die im Zusammenhang mit der Rahmenrichtlinie stehen, können dienst- bzw. arbeitsrechtliche Folgen nach sich ziehen.

Alle in dieser Rahmenrichtlinie sowie aller untergeordneten Richtlinien beschriebenen Maßnahmen dienen ausschließlich der IT-Sicherheit und des Datenschutzes. Leistungs- und Verhaltenskontrollen von Mitarbeiter:innen sind daher auf allen Ebenen (IT-Systeme, Anwendungen, Basisdienste usw.) grundsätzlich ausgeschlossen.

Dies gilt nicht, wenn Tatsachen bekannt werden, die den Verdacht einer erheblichen Verletzung der Dienst- und Arbeitspflichten oder den Verstoß gegen gesetzliche Bestimmungen begründen. Die jeweils zuständigen Mitbestimmungsgremien sowie die örtlich zuständigen Datenschutzbeauftragten sind zu beteiligen.

8.6 Leistungserbringung durch externe Dritte

Personen, Dienststellen und Unternehmen, die nicht zur Stadtverwaltung Bremerhaven gehören, für diese aber Leistungen erbringen, haben die Vorgaben der auftraggebenden Stelle zur Einhaltung der Informationssicherheitsziele gemäß dieser Rahmenrichtlinie einzuhalten.

Die auftraggebende Stelle verpflichtet die auftragnehmende Stelle in geeigneter Weise zur Einhaltung. Dazu gehört, dass die auftragnehmende Stelle bei erkennbaren Mängeln und Risiken eingesetzter Sicherheitsmaßnahmen die auftraggebende Stelle zu informieren hat.

9 Fortschreibung und Revision

Informationssicherheit ist kein unveränderlicher Zustand, sondern hängt von vielen internen und externen Faktoren ab, wie z. B. neue Schwachstellen, Bedrohungen, Gesetze oder auch der Entwicklung neuer technischer Lösungen, denen fortlaufend Rechnung getragen werden muss.

Die Akteure sind angehalten, sich an der Optimierung der Informationssicherheit zu beteiligen, sie zu unterstützen und die ständige Verbesserung des Sicherheitsniveaus anzustreben.

Verantwortlich für die Weiterentwicklung dieser Rahmenrichtlinie und der Sicherheitskonzeption ist der Lenkungsausschuss IT-Sicherheit, der Änderungen für eine neue Beschlusslage dem Magistrat der Stadt Bremerhaven vorlegt.

Die Rahmenrichtlinie zur Informationssicherheit wird fortlaufend weiterentwickelt und entweder anlassbezogen oder mindestens alle drei Jahre einer Revision unterzogen.

10 Inkrafttreten

Der Magistrat der Stadt Bremerhaven erlässt im Bekenntnis zum Stellenwert der Informationssicherheit für die Stadtverwaltung Bremerhaven die vorliegende Rahmenrichtlinie zur Informationssicherheit als grundlegende Regelung zur weitergehenden Informationssicherheit.

Die Rahmenrichtlinie zur Informationssicherheit ersetzt die Richtlinie zur Informationssicherheit für das Magistratsnetz vom 29.12.2016 in der Fassung vom 20.01.2021 und tritt am 01.01.2025 in Kraft.